

## OPERATING PROCEDURES FOR ENSURING COMPLIANCE WITH CPNI RULES

**Lenox Municipal Communications Utility** (the "Company") has implemented the following procedures to ensure that it is compliant with Part 64 of Title 47 of the Code of Federal Regulations, Subpart U – Customer Proprietary Network Information (CPNI), § 64.2001 through § 64.2011.

### Compliance Officer

The Company has appointed a CPNI Compliance Officer. The Compliance Officer is responsible for ensuring that the Company is in compliance with all of the CPNI rules. The Compliance Officer is also the point of contact for anyone (internally or externally) with questions about CPNI.

### Employee Training:

The Compliance Officer arranges for the training of employees on an annual basis, and more frequently as needed. Any new employee is trained when hired by the Company. The training includes, but is not limited to, when employees are and are not authorized to use CPNI, and the authentication methods the company is using. The detail of the training can differ based on whether or not the employee has access to CPNI.

After the training, all employees are required to sign a certification that they have received training on the CPNI rules, that they understand the Company's procedures for protecting CPNI and they understand the Company's disciplinary process for improper use of CPNI. The Company will maintain a copy of the CPNI rules in a central location so all employees have easy access to it.

Employees are instructed that if they ever have any questions regarding the use of CPNI, or if they are aware of CPNI being used improperly by anyone, they should contact the Compliance Officer immediately.

### Disciplinary Process

The Company has established a specific disciplinary process for Improper use of CPNI. The disciplinary action is based on the type and severity of the violation and could include any or a combination of the following: retraining the employee on CPNI rules, notation in the employee's personnel file, formal written reprimand, suspension or termination.

The disciplinary process is reviewed with all employees at the time of the CPNI training.

### Customer Notification and Request for Approval to Use CPNI

The Company has not asked for approval to use CPNI because it only uses CPNI in those instances where it is permissible to use CPNI without customer approval, e.g. to discuss existing services, to market enhancements to services the customer already subscribes to, as required by law, etc. It does not share the customer's CPNI with any joint venture partner, independent contractor or any other third party. For marketing campaigns, the Company does mass marketing to all customers and does not do marketing based on CPNI.

If the Company receives a call from a customer who wants to discuss services outside of the customer's existing service offerings, the customer service representative uses the oral notification for one-time use of CPNI to obtain approval for the duration of the call. The customer is told that the approval to use the CPNI is limited only to the existing call.

### Marketing Campaigns

The Company does not use any CPNI for its marketing campaigns.

### Authentication

The Company does not disclose any CPNI until the customer has been appropriately authenticated as follows:

**In-office visit** - the customer must provide a valid photo ID matching the customer's account information.

**Customer-initiated call** – the customer is authenticated by providing an answer to a pre-established question and must be listed as a contact on the account.

If the customer wants to discuss call detail information that requires a password, since the company does not use passwords, the following guidelines are followed:

- If the customer can provide all of the call detail information (telephone number called, when it was called, the amount of the call, etc.) necessary to address the customer's issue, the Company will continue with its routine customer care procedures.
- If the customer cannot provide all of the call detail information to address the customer's issue, the Company will: (1) call the customer back at the telephone number of record, (2) send the information to the address of record, or (3) ask the customer to come into the office and provide a valid photo ID.

### Notification of Account Changes

The Company promptly notifies customers whenever a change is made to the following:

- Address of record.

The notification to the customer will be made either by a Company-originated voicemail or text message to the telephone number of record or sent to the address (postal or electronic) of record.

The Company has a process for tracking when a notification is required and for recording when and how the notification is made.

### Notification of Breaches

Employees will immediately notify the Compliance Officer of any indication of a breach. If it is determined that a breach has occurred, the Compliance Officer will do the following:

- Notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) as soon as practicable, but in no event later than 7 business days after determination of the breach. The notification will be via the FCC link at <http://www.fcc.gov/eb/cpni>.
- Notify customers only after 7 full business days have passed since notification to the USSS and the FBI, unless the USSS or FBI has requested an extension.
- If there is an urgent need to notify affected customers or the public sooner to avoid immediate and irreparable harm, it will be done only after consultation with the relevant investigating agency.

- Maintain a record of the breach, the notifications made to the USSS and FBI, and the notifications made to customers. The record should include dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.
- Include a summary of the breach in the annual compliance certificate filed with the FCC.

#### Annual Certification

The Compliance Officer will file a Compliance Certification with the FCC by March 1 of each year, for data pertaining to the previous calendar year.

#### Miscellaneous

The Company takes reasonable measures to discover and protect against activity that is indicative of pretexting. Employees are instructed to notify the CPNI Compliance Officer immediately of any unusual or suspicious activity who will then determine what action needs to be taken.

#### Record Retention

The Company retains all information regarding CPNI in a secure file. Following is the minimum retention period the Company has established for specific items:

- Breaches – two years
- Annual certification – six years
- Employee training certification – two years
- All other CPNI information – two years